整数解とSchmidtの部分空間定理 (代数的整数論とその周辺)

AUTHOR(S):

平田, 典子

CITATION:

平田, 典子. 整数解とSchmidtの部分空間定理(代数的整数論とその周辺). 数理解析研究所講究録 1998, 1026: 89-103

ISSUE DATE:

1998-02

URL:

http://hdl.handle.net/2433/61767

数理解析研究所講究録
1026 巻 1998 年 89-103

整数解と Schmidt の部分空間定理

平田　典子 (日本大学理工学部数学科)

代数的整数論のシンポジウムにて 1 時間の講演の機会を与えていただいたことにまず感謝します。

K. F. Roth らの無理近似に始まり W. M. Schmidt らによって確立された部分空間定理などのディオファントス近似の方法は、高次元モーデル予想などの G. Faltings らによる数論的代数幾何学の諸問題への応用によって、その重要さが多方面に認められている。 Faltings らの問題意識は、不定方程式に対するものの近代的翻訳とも言えるが、ここではこの種のディオファントス近似が不定方程式の整数解などの問題でどういう働きをするのか、また具体的な不定方程式の整数解の問題における最近の結果等について述べてみたい。

この原稿は非専門家向けということを考えて記述した。最後の章を除いて専門家には既に良く知られていることばかりである。最近の不定方程式における様々な改良の最新情報については文献のみあげる。

1. Introduction

ディオファントス問題とは、フェルマーの大定理に代表される整数係数多変数多項式の整数解を求める問題や、その様々な拡大解釈を含むものの総称であるといえる。ディオファントス問題には近似不等式を応用するという手法が非常に有効であるが、 まず J. Liouville の定理、次いで　Roth 等の無理近似すなわち普通 Thue-Siegel-Roth の定理と呼ばれる近似不等式の復習から始めよう。

定理 1 (Liouville, 1844)

α を有理数体上 d 次の代数的数とする。このとき α によるある正定数 $c(\alpha)$ が存在して、α と異なる任意の有理数 $\frac{p}{q}$ （ただし $p, q \in \mathbf{Z}, q > 0$）に対して次が成り立つ。

$$| \alpha - \frac{p}{q} | > \frac{c(\alpha)}{q^d}$$

証明）[Schm 2] p. 114-115 を見よ。テイラー展開と通常の三角不等式を用いる証明。

系

α を有理数体上 $d \geq 2$ 次の代数的数とする。$\mu > d$ とする。このとき有理数 $\frac{p}{q}$ （ただし $p, q \in \mathbf{Z}, q > 0$）で次を満たすものは有限個しか存在しない。

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{\mu}}$$

Liouville の定理の系の有限個の有理数 $\frac{p}{q}$ は有限時間内で全部求め得る(以下少なくとも理論的には有限時間内で全部求め得る様な解のことを、effective 解と称する)。そして証明にも難しいことは使わない。しかしこの手の不等式はすべて証明が易しいと思い込むのは非常に浅はかである。次の Thue-Siegel-Roth の定理は上の定理 1 の q の指数を最良に改良しただけに見えるが、この最良指数までの改良をおこなった Roth は、この証明によりフィールズ賞を取っている。自力で 1 度でも証明しようとしてみたことのある人ならば、この定理の深さを理解できます。ただし最良指数以前の仕事の証明が Roth の定理の基礎になっていることは言うまでもなく、ノルウエーの数学者 A. Thue や C.L. Siegel, F.J. Dyson, A.O. Gel'fond たちの仕事を経て、最良なる評価に達したのである。その歴史についてはいろんな本にあるが [Schm 2] p.115 をみよ。Roth の定理以前のこれらの弱い不等式でも不定方程式に対する多くの応用はすでにある。なお α の連分数展開に関する Roth の定理と同値な結果については [Schm 1], p.13 を見よ。

定理 2 (Thue-Siegel-Roth の定理、Roth 1955)

α を有理数体上 $d \geq 2$ 次の代数的数とする。ε、C を任意の正の数とする。このとき有理数 $\frac{p}{q}$ （ただし $p, q \in \mathbf{Z}, q > 0$）で次を満たすものは有限個しか存在しない。

$$|\alpha - \frac{p}{q}| < \frac{C}{q^{2+\varepsilon}}$$

d という文字は実は定理の主張には使ってないことに注意。

定理 2 の証明は [R] または [Schm 2] p.121-150、アウトラインのみなら [Schm 1] p.16-21 および [Schm 3] p.39-41 にある。Roth の Lemma と呼ばれるところが難しい。この Lemma については最近の Faltings 、J.-H. Evertse の仕事も参照のこと [E3]。なお $C = 1$ の形で述べられているも

のもあるが、$q^{\varepsilon} \gg C$ に注意すれば、同じことである。またαが実数でないときはαの虚数部の絶対値$|\Im(\alpha)|$が$|\alpha - \frac{p}{q}|$以下であることより定理2は自明である(qを無限にとばせない)。Rothの定理の指数$2+\varepsilon$が最良なことはDirichletの引き出し論法よりわかる(M. Cugianiの仕事も参照　[Schm 1], p.13)。この指数$2+\varepsilon$はThue, Siegel, Dyson, Gel'fondと異なり、αの次数dに依らないところがすごい。

Liouvilleまではeffectiveだが、Thue以後Siegel、Dyson、Rothの定理全てineffectiveであることに注意しなければならない。つまり定理2の有限個の有理数$\frac{p}{q}$は決められない。ただし有限個である有理数の個数の上からの評価はわかる(Davenport-Roth 1955, その後多くの改良あり、[E3]参照。なおこのような数論的解がeffectiveには求まらなくても、個数の上からの評価がわかる場合はquantitativeと称することが多い)。Rothより弱いがLiouvilleよりは強い不等式でeffectiveなものとしては、A. Bakerの方法で示されたN.I. Fel'dmanの仕事などがある。

さてここでは次の不定方程式(一般にThue方程式と呼ばれるものの一部である)の整数解の有限性を、Thueの論法によって上の定理2から導いてみる。

$d \geq 3$、$m \neq 0$を有理整数とする。次のように因数分解される有理整数係数の方程式

$$(X - \alpha_1 Y) \cdots (X - \alpha_d Y) = m \cdots\cdots (1)$$

を考える。ただし$\alpha_1, \cdots, \alpha_d$は代数的数で互いに異なるとする。これを満たす整数解$X, Y \in \mathbf{Z}$が有限個であることを示そう。$Y = 0$なら自明なので$Y \neq 0$とし、方程式の両辺をY^dで割って両辺の絶対値をとる。$|Y| \geq A > 1$とすると右辺$\leq \frac{|m|}{A^d}$である。

$$\left|\frac{X}{Y} - \alpha_1\right| = \min_{1 \leq i \leq d} \left|\frac{X}{Y} - \alpha_i\right|$$

と書くと

$$\left|\frac{X}{Y} - \alpha_1\right| \leq \frac{|m|^{\frac{1}{d}}}{A}$$

である。ここで

$$\gamma = \frac{1}{2} \min_{i \neq j} |\alpha_i - \alpha_j|$$

とおくと仮定より $\gamma > 0$ である。今

$$\frac{|\, m \,|^{\frac{1}{d}}}{A} \leq \gamma$$

となるよう A を大きく取っておけば任意の $1 \leq i \leq d$ に対し

$$\left|\frac{X}{Y} - \alpha_i\right| \geq |\alpha_1 - \alpha_i| - \left|\frac{X}{Y} - \alpha_1\right| \geq 2\gamma - \gamma = \gamma$$

すなわち

$$\left|\frac{X}{Y} - \alpha_1\right| \leq \frac{|\, m \,|}{\gamma^{d-1} \,|\, Y \,|^d}$$

となり定理2における $C = \frac{|m|}{\gamma^{d-1}}$、$\varepsilon = d - 2$ の場合から $|\, Y \,| \geq A$ のときは $X, Y \in \mathbf{Z}$ が有限個であることが得られる。A はもともと m, d, α たちで書けるものなので、$|\, Y \,| < A$ のときも $Y \in \mathbf{Z}$（従って $X \in \mathbf{Z}$ も）の有限性がわかる。

この例において整数解の有限性を示すのには、Roth 程の最良評価を必要とはせず、Thue 自身の評価で十分である。Thue の評価も ineffecttive なのでこのやり方では $X, Y \in \mathbf{Z}$ の存在範囲はわからないが、Baker の effective な方法のおかげで 1967 年に上の方程式の effective な整数解の評価

$$\max(|\, X \,|, |\, Y \,|) \leq \exp((dH)^{(10d)^5})$$

（ただし H は右辺の m を含めた方程式 (1) の整数係数の絶対値の最大値）が得られた（その後 W.M. Schmidt らが Siegel の議論を使って改良）。このように近似不等式の effective version があれば、その近似不等式の応用としてわかる数論的解の effective な存在範囲も出る。Roth の評価の effective version は現在まで誰も示せていず（大問題です）、Roth の最良評価を用いないと有限性のわからない数論的解は、その存在範囲もあわせてわからないというわけである。effective な Roth の評価と同値な Baker の linear form の評価の改良版が、この数年、大予想としてあちこちで記述されていて、ちょっと見には既に証明されている Baker の linear form の評価の「積」のところが「和」に変わっただけの予想でありますが、現時点では証明の手掛かりは全くない。

2. Thue-Siegel-Roth の定理の代数体版と S-unit equation

Thue-Siegel-Roth の定理は不等式を満たす有理数の有限性ばかりでなく、代数的数の有限性も従える。以下 K を有理数体上 D 次の代数体とす

る。$M(K)$ を K の non-equivalent place の集合とし、$|\cdot|_v$ を $v \in M(K)$ に対応する通常の意味で正規化された絶対値とする。$M_\infty(K)$ を K の Archimedean place の集合とする。

$M_\infty(K) \subset S \subset M(K)$ なる有限集合 S を考え $s = \sharp S$ とおく。O_S を S 整数、すなわち $O_S = \{x \in K \mid v(x) \geq 0 \quad forall \quad v \in M(K) - S\}$、$U_S$ を S 単数、すなわち $U_S = \{x \in K \mid v(x) = 0 \quad forall \quad v \in M(K) - S\}$ とする。K_v を $|\cdot|_v$ に関する K の完備化とし、local degree を $D_v = [K_v : \mathbf{Q}_v]$ と書く。$P = (a_0, \cdots, a_n) \in \mathbf{P}_n(K)$ に対し, P の高さ $h(P)$ を

$$h(P) = \frac{1}{D} \sum_{v \in M(K)} D_v \log \max\{|\ a_0\ |_v, \cdots, |\ a_n\ |_v\}$$

と定める。$x \in K$ に対し $h(x) = h((1, x)), H(x) = \exp h(x)$ と決める。上述の高さ $h(x), H(x)$ の定義やその色々な性質はよく知られている [Si] が、大事なのは正定数 C_1、C_2 が与えられたとき、$h(x) \leq C_1$、$\deg(x) \leq C_2$ という**不等式**を満たす代数的数 x は全部 C_1、C_2 から定め得る、つまり $x = \cdots$ という**等式**を導けるという事実である。この高さといういわゆる counting function のおかげで方程式を解くという等号変形の世界に不等号を導入することが出来る。不等式というものは解析を用いて証明することができるし、不等式という弱いものを証明してそれから等式という強い主張をだせるのだから、証明手段がおおいに広がるのは言うまでもない。不定方程式に不等式を用いる理由はまずこの思想に負うている。

定理 3 (Thue-Siegel-Roth の定理の代数体翻訳版)

α を K 上 $d \geq 2$ 次の代数的数とする。K の任意の付値 $v \in M(K)$ の $K(\alpha)$ への一つの延長を再び v と書く。ε、C を任意の正の数とする。このとき代数的数 $x \in K$ で次を満たすものは有限個しか存在しない。

$$|\ \alpha - x\ |_v < \frac{C}{H(x)^{D(2+\varepsilon)}}$$

$K = \mathbf{Q}, x = \frac{p}{q}$ (ただし $p, q \in \mathbf{Z}, (p, q) = 1$) なら $H(x) = \max(|\ p\ |, |\ q\ |)$ である。$H(x)$ の指数 $D(2+\varepsilon)$ が α の K 上の次数 d に依らないところは Thue-Siegel-Roth の定理と同様である。

定理 3 から代数体の単数方程式についての大切な結果が出ることを次に示す。Siegel が 1921 年に implicit に示しており、その後少しずつ発展してきたが、ここでは単数方程式の拡張である S-Unit equation の解の個数の評価についての Evertse の著名な結果 [E1] を述べる。

定理 4 (Evertse, 1984)

S は上述の付値の有限集合、$s = \sharp S$ とする。$\alpha_1, \alpha_2 \in K - \{0\}$ とする（$\in U_S$ でなくてもよい）。この時 $\alpha_1 X + \alpha_2 Y = 1$ という方程式の $X, Y \in U_S$ 解は有限個。その個数は $\leq 3 \cdot 7^{D+2s}$。

$3 \cdot 7^{D+2s}$ という数は体次数以外 α_1, α_2 に全く依らない（この部分はEvertseの寄与で、これ以前の全ての評価の改良となり、現在でも2変数 S-Unit equation の個数評価の best known である）。そも代数体の単数は自由部分があれば無限個あるのだから、このたった一つの式でもう有限個しか解がないという事実だけでも自明でない。

有限個であることだけなら証明はつぎのようにする。Dirichlet の一般単数定理より、単数群は $U_S = \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \oplus \{Torsion\}$ となり、自由部分の階数は $s-1$ である。十分大きい $n \in \mathbf{Z}$ に対し $U_S^n = \{u^n \mid u \in U_S\}$、$U_S/U_S^n$ の位数を m とおくと $m \leq n^s$ である。$X = b_1 x^n, Y = b_2 y^n (x, y \in U_S, b_1, b_2, \cdots, b_m$ は U_S における U_S^n の coset 代表元）と表せるから、$\alpha_1 X + \alpha_2 Y = 1$ という方程式は $\alpha_1 b_1 x^n + \alpha_2 b_2 y^n = 1$ という方程式になる。この方程式は x と y の次数が同じであるからこれを因数分解した

$$\prod_{\zeta \in 1_n} \{\frac{x}{y} + \zeta \sqrt[n]{\frac{\alpha_2 b_2}{\alpha_1 b_1}}\} = \frac{1}{\alpha_1 b_1 y^n}$$

において、先の Thue 型方程式を定理2から導いた議論と同様に考えることが出来るので、ある定数 $C > 0$ が存在して

$$\left| \frac{x}{y} + \sqrt[n]{\frac{\alpha_2 b_2}{\alpha_1 b_1}} \right|_v \leq \frac{C}{|\ y\ |_v^n}$$

が言える。n は十分大とみなして良いことと、$H(\frac{x}{y}) \leq H(y)$ が $\alpha_1 b_1 x^n + \alpha_2 b_2 y^n = 1$ から従うことに注意しながら定理3を使うと、$\frac{x}{y}$ の有限性が示せる。ここで x と y の次数が同じだということから、$\frac{x}{y}$ から x と y がでる、すなわち $\alpha_1 b_1 x^n + \alpha_2 b_2 y^n = 1$ を変形した

$$y^n = \frac{1}{\alpha_1 b_1 \frac{x^n}{y^n} + \alpha_2 b_2},$$

$$x = \frac{x}{y} \cdot y$$

なる等式から x および y の有限性が従う。

$\alpha_1 X + \alpha_2 Y = 1$ という方程式の $X, Y \in U_S$ 解についてはBakerの方法で次のeffectiveな結果がわかっている（後様々な C の改良あり）。

定理5 (Baker, 1970)
$\alpha_1, \alpha_2 \in K - \{0\}$ に対し、K, S, α_1, α_2 にのみよるある正定数 C が存在して次を満たす。$\alpha_1 X + \alpha_2 Y = 1$ という方程式の $X, Y \in U_S$ 解に対し $h(X)$ （従って $h(Y)$ も）$\leq C$ である。

3. 3変数以上の S-Unit equation と Schmidt の部分空間定理

定理5は $X, Y \in U_S$ 解を理論的には具体的に求められる結果である。しかしここで同様の S-Unit equation を2変数 X, Y でなく、3変数以上で考えようとすると有限性は（成り立たないことが自明な例を除いて）証明できるが、effectiveな結果はわからないという事態に遭遇する。これは現在でもopenである。

まず3変数の S-Unit equation について、例えば $X_1 + X_2 + X_3 = 1$ を $K = \mathbf{Q}$, $S = \{2, \infty\}$ で見ると $X_3 = 1$, $X_1 = -X_2 = 2^n$ $(n \in \mathbf{Z})$ なる無限個の解を持つことに注意しよう。このように有限性の成り立たない例はあるが、これら以外の場合なら定理4の多変数版であるつぎの定理6が示せる。定理6の内容についてはE. Dubois-G. Rhin(1977)、H.P. Schlikewei-A. van der Pooerten (1982)、Evertse (1984) らの結果があるが、いずれもThue-Siegel-Roth の定理の多変数版に当たるSchmidtの著名なる部分空間定理の応用によって得られる。ここではEvertseの1995年のbest knownな評価を持ったもの [E2] を紹介しよう。

定理6 (Evertse, 1995)
$\alpha_1, \cdots, \alpha_n \in K - \{0\}$ とする。$\alpha_1 X_1 + \cdots + \alpha_n X_n = 1$ という方程式が $\sum_{i \in I} \alpha_i X_i \neq 0 \quad foreach \quad I \subseteq \{1, \cdots, n\}, I \neq \phi$ を満たすとする。このとき $X_1, \cdots, X_n \in U_S$ 解は有限個で、個数は $\leq (2^{35} n^2)^{n^3 s}$ である。

この個数の評価は $\alpha_1, \cdots, \alpha_n$ にも S の中身の各primeにも K にも依らない。特に定理4と異なり、体 K の次数 D にすらよらない。

さて、S-Unit equationの解の有限性を示す際に先のThue型の不定方程式の解の有限性に帰着させたことを思い出そう。今度は逆に、S-Unit equationの解の有限性からも、Thue型の不定方程式の解の有限性が示せる。　定理2の後に述べた(1)の不定方程式

$$(X - \alpha_1 Y) \cdots (X - \alpha_d Y) = m, \; X, Y \in \mathbf{Z}$$

を再び考える。適当に整数 A をかけて $A\alpha_1, \cdots, A\alpha_d \in O_K$ とする。ただし O_K は K の整数環とする。各因子 $L_i(X,Y) := (AX - A\alpha_i Y)\,(1 \leq i \leq d)$ は O_K で $m' := A^d m$ を割りきるから各々が m' の約数となり、$L_i(X,Y)$ は $K - \{0\}$ の U_K（O_K の単数群）に関する coset たちの有限個の和集合の内にある。さて $L_i(X,Y)\,(1 \leq i \leq d)$ は今どの 2 つも一次独立だから適当な $\beta_1, \beta_2 \in K - \{0\}$ が存在して

$$\beta_1 \frac{L_1(X,Y)}{L_3(X,Y)} + \beta_2 \frac{L_2(X,Y)}{L_3(X,Y)} = 1 \cdots\cdots (2)$$

とできる（実際は $L_i(X,Y)$ たちのなかの 3 個が、どの 2 つずつも一次独立をみたすという仮定で十分なのである）。先の $K - \{0\}$ の U_K に関する coset の代表元をくりこむと、有限種類しか動かない $\beta_1', \beta_2' \in K - \{0\}$ を係数とする単数方程式として (2) をみなすことが出来る。各々の β_1', β_2' に対して再び有限個しか (2) が単数解を持たないのは定理 4 で見たとおりなので、$\dfrac{L_1(X,Y)}{L_3(X,Y)} = u_1, \dfrac{L_2(X,Y)}{L_3(X,Y)} = u_2$ で $u_1, u_2 \in K$ が成り立つ（u_1, u_2 は単数と K の元の積で有限個しか動かない）。これより X, Y は定数倍を除いて求まるが、その定数ももとの (1) の不定方程式から定まる。以上のようにして (1) の Thue 型の不定方程式の整数解の有限性が従う。

Baker の示した、整数係数の楕円曲線上に整数点が有限個しかないという結果についても、楕円曲線の式を Unit の話に帰着させて示す。楕円曲線の式や (1) の式は 2 変数だから 2 変数の Unit equation で良い。従って定理 5 から effective な結果もわかるのである。

多変数の S-Unit equation からは多変数の Thue 型にあたる Decomposable form equations などの不定方程式の解の有限性が得られる。これについてはたとえば [E-G] を見よ。しかし 3 変数以上の S-Unit equation には Baker の手法をうまく適用できないため effective な評価がないので、Decomposable form equations については一般的な effective な結果はない（部分的なものなら多変数 Decomposable form equations でも effective な結果が S.V. Kotov, K. Győry らによって求められている）。

多変数の S-Unit equation の解の有限性の証明には W.M. Schmidt の部分空間定理を使うが、部分空間定理は Thue-Siegel-Roth の定理の多変数版であり、Roth の最良評価をそのまま踏襲できて最良の exponent を持っている。しかし Roth の定理が effective にできないので部分空間定理もそのまま ineffective である。部分空間定理の完全に一般的な effective 版

は証明不可能であろうと言う予想もある(M. Mignotte)。部分空間定理の1996年のD. Roy-J.L. Thunderの仕事や応用についての最近の発展については[E-Schl]などをみよ。

さてここでSchmidtの部分空間定理（定性的）を記述することにする。部分空間定理には代数体への拡張、付値の部分を有限個の$v \in S$についての積の形にしたもの、以下述べる例外部分空間の個数を評価したものなどがある（定量的部分空間定理と称する、Schmidtが最初に成功しp-adic版についてのSchlikeweiの仕事などを経て現在のbest knownは[E3]の評価)。

証明の複雑さ長さは授業でやる場合、Rothの定理なら2コマ、定性的部分空間定理なら集中講義1回、定量的部分空間定理なら毎週1コマで1年という具合である。

定理7 (Schmidt, 1972 [Schm3] p.176)

$n \geq 2, n \in \mathbf{Z}$とする。変数$X_1, \cdots, X_n$をもつ$K$係数の1次独立な1次式$L_1, \cdots, L_n$を考える。$\mathbf{X} = (X_1, \cdots, X_n) \in \mathbf{Z}^n$に対し、$\mid \mathbf{X} \mid = \sqrt{X_1^2 + \cdots + X_n^2}$とおく。$\varepsilon$を任意の正の数とする。このとき

$$|L_1(\mathbf{X}) \cdots, L_n(\mathbf{X})| < \frac{1}{\mid \mathbf{X} \mid^{\varepsilon}}$$

を満たす$\mathbf{X} = (X_1, \cdots, X_n) \in \mathbf{Z}^n - \{0\}$は有限個のproper linear subspaces of $\mathbf{Q}^n$に含まれる、すなわち$\mathbf{X} \in T_1 \cup \cdots \cup T_t$, $t < \infty$。

ここでlinear subspaceとは通常のベクトル部分空間である。tの評価は[E3]にあるが、評価式は$n, \varepsilon, D = [K : \mathbf{Q}]$でかける部分と1次式$L_1, \cdots, L_n$の係数の高さで書ける部分にわかれてそれぞれexplicitなものがある。

4. Padé近似と1つの指数方程式

変数が3以上の場合、不定方程式の解はかならずしも理想的には扱えていないが、それでもいくつかずつ単発の結果がある。ここでは4変数の次のような問題を考えてみよう。

問題8 (T.N. Shorey-R. Tijdeman、現時点でopen)

$$\frac{x^m - 1}{x - 1} = y^q \cdots\cdots (3)$$

を4個の未知数 $x,y,m,q \in \mathbf{Z}, x>1, y>1, m>2, q>1$ について解くとき、解は3つしか存在しない。

(3) 式で知られている解は

$$(x,y,m,q) = (3,11,5,2),(7,20,4,2),(18,7,3,3)$$

であるから、問題8はこれ以外に解がないことを言っている。1943年にW. Ljunggren [Lj] が (3) の $q=2$ の場合は $x=3, y=11, m=5$、$x=7, y=20, m=4$ しか解のないことを示した。以下 q は奇素数として構わない。Shorey-Tijdeman はある条件下で (3) の全ての解が effective に決めうることを示した [Sh-T]。しかしその条件は x を固定するか、または m が決まった素因数を持つ場合というもので、制約は大きい。K. Inkeri らの結果 [I] もあるが、ここでは少し条件をかえて、次の問題を考える。

問題9

$$\frac{x^m-1}{x-1} = y^q$$

を4個の未知数 $x,y,m,q \in \mathbf{Z}, x>1, y>1, m>2, q>1$ について解くとき、x が累乗の形をしているもの、つまり $x=z^\mu, z, \mu \in \mathbf{Z}, z>1, \mu>1$ となる整数解は有限個で、全て決定できる。

N. Saradha と Shorey [Sa-Sh] は問題9について x が2乗数 つまり $\mu=2$ なら解は有限個であることを証明した（no solution とアナウンスされたが解なしを言うために用いた M.-H. Le の補題が誤っており、直せなかったため、有限個に留まった）評価は effective にできうるが、求められていない。以下 μ は奇素数としてよい。さてここでは一般の累乗数、つまり任意の μ について次のような解の有限性が示せた。

定理10 (H-Shorey, 1997 [H-Sh])

$$\frac{x^m-1}{x-1} = y^q$$

を $x,y,m,q \in \mathbf{Z}, x>1, y>1, m>2, q>1$ with $x=z^\mu, z, \mu \in \mathbf{Z}, z>1, \mu>1$ で考えるとき、$q > 2(\mu-1)(2\mu-3)$ ならば、整数解は有限個で、$\max\{x,y,m,q\}$ は μ で書ける effective な定数で上から評価される。

系

$q \neq 5,7,11$ のとき、定理10の式の $x = cube$ なる整数解 x,y,m,q は有限個で、effective に決定しうる。

4乗数、5乗数、$\cdots$ についても同様。

この証明にはPadé近似と呼ばれる手法による近似不等式を用いる。正しくはPadéによる無理数の有理数による近似の方法をもとにしたBakerの方法[B1]によって示せる。補題1 1のその近似不等式はYu.V. NesterenkoとShoreyの論文[Sh-N]の補題のある改良にあたる。

補題1 1 ([H-Sh])

A, B, K, n を $A > B, K < n, n \geq 3, \omega := (B/A)^{1/n} \in \mathbf{R} - \mathbf{Q}$ なる正整数とする。$0 < \phi < 1$ に対し次の数を定める。

$$\delta = 1 + \frac{2-\phi}{K},\ s = \frac{\delta}{1-\phi},$$

$$u_1 = (3^{2K+1} \cdot 2^{s(4K+2+3n(K+1))+(1+(3n)/2)(K+1)})^{1/(Ks-1)},$$

$$u_2^{-1} = 3^{2K+1} K^2 (1+2^{-29})^{K-1} n^{2K} 2^{K+s+2+3n(K+1)}$$

これらの数が

$$A(A-B)^{-\delta} u_1^{-1} > 1$$

を満たすとする。この時全ての整数 p、q （ただし $q > 0$）に対し次が成立する。

$$\left| \omega - \frac{p}{q} \right| > \frac{u_2}{Aq^{K(s+1)}} \cdots\cdots (4)$$

ここで(4)の不等式は全ての有理数 $\frac{p}{q}$ について成り立つ。Rothの定理の主張が

$$| \alpha - \frac{p}{q} | \geq \frac{C}{q^{2+\varepsilon}}$$

が有限個の例外（具体的にはわからないineffectiveな例外集合）を除いた有理数 $\frac{p}{q}$ について成り立つと言っていることと比べると、exponentの $K(s+1)$ は悪いが、例外集合がないので、effectiveになっている。（不等式の右辺の u_2, A はeffective性には影響ない）。ただし $\alpha = \omega$ の時に限る。またBakerのもとの近似では上の $\delta = 2$ としかとれないが、その仮定は弱まっているため定理1 0に応用できる形になっている（$\delta = 2$ とすると定理1 0の証明はうまくいかない）。

補題１１の証明

$$l(r) = n^{2K}(r+1)^{2K+1} r^{2K+1} A^r 2^{3n(r+1)(K+1)/2+r(K+1)},$$

$$\lambda_1 = 3^{2K+1} A \cdot 2^{(K+1)((3n)/2+1)},$$

$$\lambda_2 = 2^{4K+2+3n(K+1)}(A-B)^{K+1} A^{-K},$$

$$c = 2^{3n(K+1)/2} n^{2K},$$

$$\Lambda = \frac{\log\ \lambda_1}{\log\ \lambda_2}$$

とおく。$0 < \phi < 1$ から $0 < \lambda_2 < 1, s > 1, 0 < -\Lambda \leq s$ がわかる。$m_j = j$ $(0 \leq j \leq K)$ として [B1] の Lemma 4 と Lemma 5 の方法を踏襲すると、整数 r, p, q（ただし $r > 0$, $q > 0$ 、$p \neq q$） に対し次の４条件を満たす多項式 $P_r(X) \in \mathbf{Z}[X]$ が存在することがわかる: (i) $\deg P_r \leq K$, (ii) $H(P_r) \leq l(r)$, (iii) $P_r(\frac{p}{q}) \neq 0$, (iv) $|P_r(\omega)| \leq \lambda_2^r$

ここで $H(P_r)$ は P_r の係数の絶対値の最大値である（通常の高さ）。また $p = q$ のときは補題は自明である。$|\omega - p/q| < 2^{-29}$ としてよいことにも注意する。r を次を満たす最小整数とする:

$$\lambda_2^r \leq \frac{1}{2q^K}$$

ここで $l(r) \leq c\lambda_1^r$ がわかる。$r \geq 2$ として $\lambda_2^r > \frac{\lambda_2}{2q^K}$ から

$$l(r) \leq c\lambda_1^r = c\lambda_2^{r\Lambda} \leq c\left(\frac{\lambda_2}{2q^K}\right)^{\Lambda} = c\lambda_1 2^{-\Lambda} q^{-K\Lambda} \leq c\lambda_1 2^s q^{Ks}$$

が得られる。

$r = 1$ のときは $l(r) \leq c\lambda_1 2^s q^{Ks}$ がなりたつ。さらに

$$\frac{1}{q^K} \leq \left|P_r\left(\frac{p}{q}\right)\right| \leq \left|P_r\left(\frac{p}{q}\right) - P_r(\omega)\right| + |P_r(\omega)|$$

$$\leq \left|P_r\left(\frac{p}{q}\right) - P_r(\omega)\right| + \frac{1}{2q^K}$$

がいえるから、

$$\left|P_r\left(\frac{p}{q}\right) - P_r(\omega)\right| \geq \frac{1}{2q^K}$$

が導かれる。一方

$$\left|P_r\left(\frac{p}{q}\right)-P_r(\omega)\right|=\left|\int_{p/q}^{\omega}P_r'(X)dX\right|$$

$$\leq K^2(1+2^{-29})^{K-1}l(r)\left|\omega-\frac{p}{q}\right|$$

であるから

$$\left|\omega-\frac{p}{q}\right|>\frac{u_2}{Aq^{K(s+1)}}$$

が u_2 の定義より従う。補題１１の証明終。

定理１０の証明の概要

問題９の不定方程式で $x=z^\mu$ なるものにおいて $\max(x,y,m)$ が q と μ にのみよる effectively computable number で上から評価されることを補題１１から示す。その後 q が bounded であることを示すには、Baker の linear forms in logarithms を使えばよい。

$\max(x,y,m)$ が上から押さえられないと仮定すると、初等的議論から (cf. Lemma 2 [H-Sh], これは Shorey に負う)

$$y=y_1y_2,y_1,y_2\in\mathbf{Z},y_1>1,y_2>1,(y_1,y_2)=1$$

$$(z-1)y_1^q=z^m-1,\ (z^{\mu-1}+\cdots+1)\,y_2^q=z^{m(\mu-1)}+\cdots+1$$

となる。このとき

$$0<(z^{\mu-1}+\cdots+1)y_2^q-(z-1)^{\mu-1}y_1^{q(\mu-1)}\leq\mu z^{m(\mu-2)}$$

なので

$$0<\left|\omega-\frac{y_2}{y_1^{\mu-1}}\right|<\frac{2\mu z^{m(\mu-2)}}{z^{\mu-1}y_1^{q(\mu-1)}}\quad\cdots\cdots(5)$$

が得られる。 ここで

$$\omega=\left(\frac{(z-1)^{\mu-1}}{z^{\mu-1}+\cdots+1}\right)^{1/q}$$

としている。補題１１を $A=z^{\mu-1}+\cdots+1$, $B=(z-1)^{\mu-1}$, $n=q\geq3$, $K=2(\mu-2)<q$, $\phi=\mu^{-4}$, $\delta=(\mu-1-(\phi/2))/(\mu-2)$, $s=\delta/(1-\phi)$, $p=y_2$, $q=y_1^{\mu-1}$ として使うと、定理１０の仮定 $q>2(\mu-1)(2\mu-3)$ から

$$K(s+1)(\mu-1)/q = \frac{(2-\phi)(K+1)(\mu-1)}{(1-\phi)q} < 1-\mu^{-4} \qquad \cdots\cdots(6)$$

が従う。補題１１の仮定は

$$z^{\mu-1}(\mu z^{\mu-2})^{-\delta}u_1^{-1} > 1$$

ならば満たされるが、これは十分大きい c_1 に対し $z \geq c_1$ であることからOKなので、補題１１が使えてその結論より

$$\left|\omega - \frac{y_2}{y_1^{\mu-1}}\right| > \frac{u_2}{2z^{\mu-1}y_1^{K(s+1)(\mu-1)}} \cdots\cdots(7)$$

がでる。上からの評価 (5) と下からの評価 (7) をぶつけると、

$$\frac{1}{\mu-1} \leq \frac{K(s+1)}{q} + \frac{1}{\mu^5}$$

が従い、不等式 (6) に矛盾する。

References

[B1] A. Baker, Simultaneous rational approximations to certain algebraic numbers, *Proc. Cambridge Philos. Soc.*, **63** (1967), 693–702.

[B2] A. Baker, *Transcendental Number Theory*, Cambridge Math. Library, Cambridge UP (1975).

[E1] J.-H. Evertse, On equations in S-units and the Thue-Mahler equation, *Invent. Math.*, **75** (1984), 561-584.

[E2] J.-H. Evertse, The number of solutions of decomposable form equations, *Invent. Math.*, **122** (1995), 559-601.

[E3] J.-H. Evertse, An improvement of the quantitative Subspace theorem, *Compositio Math.* **101** (1996), 225–311.

[E-G] J.-H. Evertse and K. Győry, The number of families of solutions of decomposable form equations, *Acta Arith.*, **80** (1997), 367-394.

[E-Schl] J.-H. Evertse and H.P. Schlickewei, A quantitative version of the absolute subspace theorem, In preparation.

[F1] G. Faltings, Endlichkeitssätze für abelsche Varietätet über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366, ibid. **75** (1984), 381.

[F2] G. Faltings, Diophantine Approximation on Abelian Varieties, *Ann. Math.* **129** (1991), 549–576.

[H-Sh] N. Hirata-Kohno and T.N. Shorey, The equation $(x^m-1)/(x-1) = y^q$ with x power, in *Analytic Number Theory*, ed. Y. Motohashi, London Math. Society Lecture Note Series **247**, Cambridge UP (1997), 119-126.

[I] K. Inkeri, On the diophantine equation $a(x^n-1)/(x-1) = y^m$, *Acta Arith.*, **21** (1972), 299-311.

[La] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag (1983).

[Lj] W. Ljunggren, Noen setninger om ubestemte likninger av formen $(x^n-1)/(x-1) = y^q$, *Norsk. Mat. Tidsskr.* (1), **25** (1943), 17–20.

[R] K. F . Roth, Rational approximations to algebraic numbers, *Mathematika* **2**, 1955, 1–20.

[Schm1] W. M. Schmidt, *Approximation to algebraic numbers*, Monographie **19** de L'Enseignement Mathématique (1972).

[Schm2] W. M. Schmidt, *Diophantine Approximations*, Lecture Notes in Math. **785** (1980), Springer-Verlag.

[Schm3] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. **1467** (1991), Springer-Verlag.

[Sa-Sh] N. Saradha and T.N. Shorey, The equation $(x^n-1)/(x-1) = y^q$ with x square, *Acta Arith.*, (1996).

[Sh-N] T.N. Shorey and Yu.V. Nesterenko, Perfect powers in products of integers from a block of consecutive integers II, *Acta Arith.*, **76** (1996), 191-198.

[Sh-T] T.N. Shorey and R. Tijdeman, New Applications of Diophantine approximation to Diophantine equations, *Math. Scand.*, **39** (1976), 5-18.

[Si] J.-H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106** (1986), Springer-Verlag.